(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 874 503 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.10.1998 Bulletin 1998/44

(51) Int Cl.[6]: **H04L 29/06**

(21) Application number: **98303004.0**

(22) Date of filing: **20.04.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.04.1997 JP 106105/97**

(71) Applicant: **SONY CORPORATION**
Tokyo 141 (JP)

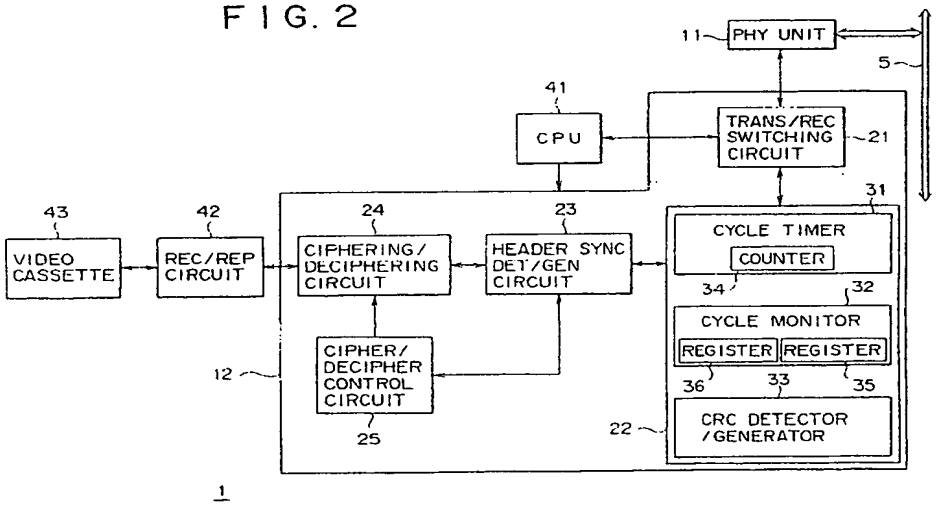
(72) Inventors:
- **Osakabe, Yoshio, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Sato, Makoto, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Osawa, Yoshitomo, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Asano, Tomoyuki, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Ishiguro, Ryuji, c/o Sony Corporation**
  Shinagawa-ku, Tokyo 141 (JP)
- **Shima, Hisato**
  Saratoga, California 95070 (US)

(74) Representative: **Pilch, Adam John Michael**
D. YOUNG & CO.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Data transmitting and/or receiving apparatus, methods and systems for preventint illegal use of data

(57) Data to be transmitted via a serial bus (5) in conformity with the IEEE 1394 protocol are ciphered by a ciphering/deciphering circuit (24), and headers are attached thereto by a header sync detecting/generating circuit (23). After further attachment of a CRC code by a CRC detector/generator (33), the data are packetized into isochronous packets of an isochronous mode by a transmission/reception switching circuit (21), whereby transmission of the data can be performed with enhanced security. Out of the cipher keys employed, a session key invariable in each session of the data is transmitted in each packet of an asynchronous mode, and a time variable key updated in each session is transmitted in each packet of an isochronous mode. The ciphered data obtained by depacketizing the packets of the isochronous mode are deciphered, so that the data transmitted with security can be deciphered exactly, and thus illegal use of the data can be prevented.

FIG. 2



EP 0 874 503 A2

Description

The present invention relates to a data transmitting apparatus and method, a data receiving apparatus and method, and a data transmitting/receiving system and method, and more particularly to those for preventing illegal use of data in transmitting and/or receiving the data.

Recently, there has been widespread application of the IEEE 1394 high performance serial bus (hereinafter referred to simply as 1394 bus) standardized by the IEEE. In such 1394 bus, digital video and audio signals can be transmitted fast together with control commands in real time via a single cable by connecting thereto electronic apparatus such as audio-visual (AV) apparatus and a personal computer.

In transmission of data via a 1394 bus, there are known an asynchronous mode (asynchronous data transmission mode) and an isochronous mode (synchronous data transmission mode) where the data are synchronous with isochronous cycles of 8 kHz (125 μs) generated by a cycle master in the 1394 bus. Commands are transmitted generally in an asynchronous mode, while video and audio signals are normally transmitted in an isochronous mode due to the necessity of real time reproduction.

However, data transmission in the isochronous mode is performed through multi-address communication where a destination of the data is not specified. For this reason, when any video or audio signal to be protected with respect to the copyright is transmitted via a 1394 bus, there arises a problem in that some users not permitted by the relevant copyrighter may copy such video or audio signal illegally or may change or modify the copied signal.

It is therefore an aim of at least an embodiment of the present invention to realize exact prevention of any illegal use of such data.

According to a first aspect of the present invention, there is provided an apparatus for transmitting data in a first or asynchronous mode and a second or isochronous mode. This apparatus comprises a means for ciphering the data to be transmitted by the use of cipher keys; a means for packetizing the ciphered data into packets of the isochronous mode; and a means for transmitting the output of the packetizing means. In this apparatus, transmission of the data is performed in conformity with the IEEE 1394 protocol, and the packetizing means attaches, to a header of the ciphered data, an identification code relative to the ciphering. The cipher keys consist of a session key invariable in each session of the data to be transmitted, and a time variable key updated in each session. Information relative to the time variable key is contained in each packet of the isochronous mode, and information relative to the session key is also contained therein.

According to a second aspect of the present invention, there is provided a method of transmitting data in a first or asynchronous mode and a second or isochronous mode. This method comprises the steps of ciphering the data to be transmitted by the use of cipher keys; packetizing the ciphered data into packets of the isochronous mode; and transmitting the packetized output. In this system, transmission of the data can be executed with enhanced security.

According to a third aspect of the present invention, there is provided an apparatus for receiving data transmitted thereto in a first or asynchronous mode and a second or isochronous mode. This apparatus comprises a means for receiving the transmitted data; a means for depacketizing the output packets obtained from the receiving means; and a means for deciphering the ciphered data outputted from the depacketizing means. In this apparatus, transmission of the data is performed in conformity with the IEEE 1394 protocol, and the depacketizing means separates an identification code relative to the ciphering from the received data. The cipher keys consist of a session key invariable in each session of the data to be transmitted, and a time variable key updated in each session. Information relative to the time variable key is contained in each packet of the isochronous mode, and information relative to the session key is also contained therein. Therefore, the data transmitted with security can be deciphered exactly.

And according to a fourth aspect of the present invention, there is provided a method of receiving data transmitted in a first or asynchronous mode and a second or isochronous mode. This method comprises the steps of receiving the transmitted data; depacketizing the output packets obtained in the receiving step; and deciphering the ciphered data outputted in the depacketizing step.

Thus, it is possible to realize improvements in transmission and reception of the data with enhanced security.

The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

Fig. 1 is a block diagram showing a structural exemple of a data transmitting/receiving system to which the present invention may be applied;
Fig. 2 is a block diagram showing an internal structural example of a digital video cassette recorder in Fig. 1;
Fig. 3 is an explanatory diagram showing the timing of data transmitted via a 1394 bus;
Fig. 4 shows a format of an isochronous packet;
Fig. 5 shows a format of a CIP header; and
Fig. 6 shows a format of a cycle start packet.

Hereinafter some preferred embodiments of the present invention will be described in detail with reference to the accompanying drawings.

Fig. 1 shows a structural example of an information

processing system where the present invention is applied. This system comprises a digital video cassette recorder 1, a television receiver 2, a personal computer 3 and a DVD player 4 which are connected mutually via a 1394 bus 5.

Fig. 2 shows an internal structural example of the digital video cassette recorder 1. A PHY unit 11 receives input data transmitted thereto via a 1394 bus 5 and, after demodulating the same, outputs the demodulated data to a transmission/reception switching circuit 21 in a link unit 12. Further the PHY unit 11 demodulates data supplied from the transmission/reception switching circuit 21 to be transmitted, and then outputs the modulated data to the 1394 bus 5.

The transmission/reception switching circuit 21 in the link unit 12 separates the input signal from the PHY unit 11 into packets of an asynchronous mode and packets of an isochronous mode and, after depacketizing the asynchronous-mode packets, outputs the same to a CPU 41. Further the switching circuit 21 depacketizes the isochronous-mode packets and then outputs the same to a timing circuit 22. The asynchronous-mode signal supplied from the CPU 41 is packetized, while the data supplied from the timing circuit 22 are packetized into packets of the isochronous mode and then are outputted to the PHY unit 11.

The timing circuit 22 includes a cycle timer 31, a cycle monitor 32 and a CRC detector/generator 33. The cycle timer 31 has a counter 34 therein. The counter 34 counts predetermined clock pulses and generates a count value which represents the timing of an isochronous cycle of 125 μs. The cycle monitor 32 includes registers 35 and 36. In the register 35, there is held the destination offset value recorded in the cycle start packet transmitted via the 1394 bus. Meanwhile in the register 36, there is held the value of cycle time data of the cycle start packet.

The CRC detector/generator 33 detects CRC data for error detection and correction from the received data, and then executes a process of error detection and correction by the use of such CRC data. In transmission of the data, the CRC detector/generator 33 executes a process of attaching the CRC data to the data to be transmitted.

At the data reception time, the header sync detecting/generating circuit 23 detects the header and the sync from the data supplied thereto from the timing circuit 22 and, after separating the same, outputs the real data part to the ciphering/deciphering circuit 24. And at the data transmission time, the circuit 23 attaches the header and the sync to the data supplied to the ciphering/deciphering circuit 24 to be transmitted, and then outputs the same to the timing circuit 22.

At the data reception time, the ciphering/deciphering circuit 24 deciphers the supplied data from the header sync detecting/generating circuit 23 under control of the cipher/decipher control circuit 25, and then outputs the deciphered data to the recording/reproducing circuit 42. And at the data transmission time, the circuit 24 ciphers the input data from the recording/reproducing circuit 42 under control of the cipher/decipher control circuit 25, and then outputs the ciphered data to the header sync detecting/generating circuit 23. The cipher/decipher control circuit 25 controls the header sync detecting/generating circuit 23 to attach predetermined identification data to the header or the data, or to extract the same. Further the cipher/decipher control circuit 25 controls the operation of the ciphering/deciphering circuit 24.

At the data reception time, the recording/reproducing circuit 42 modulates the input data from the ciphering/deciphering circuit 24 and then records the modulated data in a video cassette 43. And in a reproduction mode, this circuit 42 reproduces the data recorded in the video cassette 43 and, after demodulating the reproduced data, outputs the same to the ciphering/deciphering circuit 24.

Fig. 3 shows the timing of data transmitted to the 1394 bus 5. Suppose now that, for example, the digital video cassette recorder 1 reproduces the data from the video cassette 43 and transmits the reproduced data to the television receiver 2. It is also supposed here that the DVD player 4 transmits the data, which have been reproduced from a loaded DVD (disk), to the personal computer 3 via the 1394 bus 5. In this example, it is further supposed that a signal stream A is reproduced from the video cassette 43 and is outputted from the digital video cassette recorder 1, while a signal stream B is reproduced from the DVD and is outputted from the DVD player 4.

Suppose now that the cycle master of the 1394 bus 5 is the digital video cassette recorder 1 for example. In this case, the CPU 41 controls the transmission/reception switching circuit 21 to generate cycle start packets for specifying the 125 μs isochronous cycles of the 1394 bus 5. The cycle start packets are arrayed as S_1, S_2, ... at the heads of isochronous cycles, as shown in Fig. 3.

As will be described later with reference to Fig. 6, cycle time data are arrayed in the cycle start packet. The count value obtained from the counter 34 of the cycle timer 31 is recorded in the cycle time data. Any electronic apparatus other than the cycle master connected to the 1394 bus 5 reads out the cycle time data and holds the same in the register of the internal cycle monitor.

For example, when the cycle master is the personal computer 3 instead of the digital video cassette recorder 1, the personal computer 3 transmits cycle start packets. In this case, the digital video cassette recorder 1 receives, in its PHY unit 11, the cycle start packet transmitted thereto via the 1394 bus 5, and then depacketizes the received packet in its transmission/reception switching circuit 21. Thereafter the depacketized data are inputted to the timing circuit 22. Subsequently in the timing circuit 22, the cycle time data contained in the cycle start packet are read out by the cycle monitor 32, and the read value is held in the register 36. And then, time man-

agement of the isochronous cycles on the 1394 bus 5 is performed with reference to the value thus held in the register 36.

In this manner, the time bases of isochronous cycles of the electronic apparatus connected to the 1394 bus 5 are rendered common.

Since the digital video cassette recorder 1 and the DVD player 4 are currently transmitting data via the 1394 bus 5, time slots are allocated thereto at predetermined timing of each isochronous cycle in a manner to enable transmission of isochronous packets. Each of the digital video cassette recorder 1 and the DVD player 4 compresses and packetizes the signal stream A or B, and then transmits the packetized data at the timing of the time slot allocated thereto.

For example, the digital video cassette recorder 1 reproduces the video cassette 43 in its recording/reproducing circuit 42, and then supplies the reproduced data to the ciphering/deciphering circuit 24 for ciphering the data by the use of cipher keys which consist of a session key S and a time variable key i. The ciphered data are supplied to the header sync detecting/generating circuit 23, where the data are compressed and a header is attached thereto. The header-attached data thus obtained are inputted to the timing circuit 22, where a CRC code is further attached to each of the header and the data part.

The data outputted from the timing circuit 22 are supplied to the transmission/reception switching circuit 21 and then are packetized into a packet of the isochronous mode. As described, this packet is transmitted from the PHY unit 11 via the 1394 bus 5 at the timing of the allocated time slot.

Such a process is executed per isochronous cycle as shown in Fig. 3, and signals A_1, A_2, A_3, ... of a signal stream A are transmitted as packets, which are denoted by the same reference symbol, at the timing of predetermined time slots of individual isochronous cycles. In any isochronous cycle where none of data to be transmitted is existent, empty packets a_1, a_2 are transmitted. In each empty packet, merely a header is existent without any real data part.

An operation similar to the above is performed in the DVD player 4 also, so that signals B_1, B_2, ... of a signal stream B are transmitted as packets, which are denoted by the same reference symbol, at the timing different from the signal stream A.

For example, when the CPU 41 transmits a command, the command is inputted to the transmission/reception switching circuit 21. Then this circuit 21 packetizes the command into a packet of the asynchronous mode and transmits the same as C_1, C_2 or the like, as shown in Fig. 3.

Such asynchronous packet is transmitted in accordance with requirement, and is not generated always in each isochronous cycle.

Similarly, as will be described later, the CPU 41 transmits a session key S, which is one of cipher keys, in an asynchronous packet.

In this manner, the signal stream A transmitted via the 1394 bus 5 is received by the television receiver 2, while the signal stream B is received by the personal computer 3. Suppose now that, for the sake of explanatory convenience, the signal stream A is received by the digital video cassette recorder 1 shown in Fig. 2. In this case, the following operation is performed.

The PHY unit 11 receives the packets transmitted thereto via the 1394 bus 5 and then supplies the same to the transmission/reception switching circuit 21. Subsequently, this switching circuit 21 separates the input packets into isochronous packets and asynchronous packets, then depacketizes the isochronous packets and outputs the data to the timing circuit 22. The circuit 21 depacketizes the asynchronous packets also and outputs the data to the CPU 41. As a result, for example, the signal stream A is supplied to the timing circuit 22, while the command and the session key S are supplied to the CPU 41.

The CRC detector/generator 33 in the timing circuit 22 supplies the input data to the header sync detecting/generating circuit 23. Subsequently the CRC detector/generator 33 detects the CRC code from the data supplied thereto from the header sync detecting/generating circuit 23, and then executes a process of error detection and correction by the use of such CRC code. Thereafter the error-corrected data are returned to the header sync detecting/generating circuit 23.

The header sync detecting/generating circuit 23 separates the header from the input data and supplies the header information to the cipher/decipher control circuit 25 while supplying the real data part to the ciphering/deciphering circuit 24. The cipher/decipher control circuit 25 detects ciphering identification data included in the header detected by the header sync detecting/generating circuit 23, and then controls the ciphering/deciphering circuit 24 in accordance with the result of such detection. More specifically, when the identification data signifies that the data are ciphered, the control circuit 25 enables the ciphering/deciphering circuit 24 to execute a deciphering process by the use of the cipher key. But when the identification data signifies that the data are not ciphered, such deciphering process is omitted.

The data outputted from the ciphering/deciphering circuit 24 are modulated in a predetermined mode by the recording/reproducing circuit 42 and then are supplied to the video cassette 43 to be recorded therein.

In the embodiment of this invention, cipher keys employed for ciphering and deciphering the data in the ciphering/deciphering circuit 24 consist of a session key S and a time variable key i. The session key S is updated per session (e.g., per movie information or per reproduction). In other words, the session key S has an invariable value within one session, whereas the time variable key i is updated frequently in each session. Thus, higher security can be achieved by the use of a session key S and a time variable key i as cipher keys.

More specifically, even if the session key S is pirated, it is impossible to decipher the ciphered data in case the time variable key i is unknown. Further, even if the time variable key i is also pirated, since the time variable key i is updated every moment, the data are decipherable merely for an extremely short period of time but are rendered not decipherable any longer thereafter.

The session key S is transmitted at predetermined timing in an asynchronous packet, as denoted by K_1, K_2 in Fig. 3. However, as will be described later, it is a matter of course that the session key S can be transmitted in an isochronous packet similarly to the time variable key i.

Fig. 4 shows a format of an isochronous packet. As represented in this diagram, first two quadlets are used as an isochronous header. A data length is recorded at the top of this header, and next is recorded a tag which indicates whether a CIP header is attached or not in a data field. Thereafter a channel is disposed next to the tag. This channel is used to identify, for example, a stream A or a stream B in Fig. 3.

In Fig. 4, "tcode" (transaction code) prescribes the format of a packet. In the case of an isochronous start packet, it is set to 1010 (= A). Next "sy" denotes a synchronization code which is prescribed per application. In the embodiment of this invention, two bits of the time variable key i composed of 32 to 40 bits are disposed in the two lower-order bits of the synchronization code "sy". For example, when the time variable key i is composed of 32 bits, a total of 16 packets completely constitute the time variable key i. A flag, which signifies that the relevant packet is the top one or not of the time variable key i, can be attached to the third bit from the LSB of the code "sy". For example, this third bit is set to 1 in case the relevant packet is the top one of the time variable key i, or it is set to 0 in the other case.

when the time variable key i is recorded as described in the synchronization code "sy", a value 1100 (= C) may be set in "tcode" to serve as an identification code of the time variable key i.

The cipher/decipher control circuit 25 collects two bits of the time variable key i in each packet from the header information outputted from the header sync detecting/generating circuit 23 and, upon termination of collecting such bits of 16 packets, transfers the completed time variable key i to the ciphering/deciphering circuit 24.

As shown in Fig. 4, the second quadlet of the isochronous header is used as a header CRC. And a CIP header corresponding to two quadlets is disposed in the next data field of the isochronous header, and contents are disposed thereafter. The contents represent ciphered data, as described above.

According to the MPEG standard, a source header is disposed in the area of such contents. In this case, any source header with a time stamp or the like recorded therein is not ciphered.

Data CRC is disposed next to the data field.

Fig. 5 shows a detailed structure of a CIP header. As represented in this diagram, a bit (= 0) signifying the top of the header is disposed at the top thereof in the first CIP header 1 out of headers of two quadlets, while a bit 1 is disposed in the second CIP header 2. More specifically, the first bit serves as "EOH_n" (End of CIP header) signifying whether this quadlet is the last or not of the CIP header. This value is set to 0 when any other quadlet follows, or to 1 when it is the last quadlet of the CIP header.

The second bit serves as "Form_n" which represents, in combination with "EOH", the quadlet of the CIP header field. In the embodiment of the present invention, this bit is set to 1 in the case of ciphered data, or to 0 in the case of non-ciphered data.

The third to eighth bits of the CIP header 1 serve as "SID" (Source node ID), and "DBS" (Data block size in quadlets) is disposed next to "SID". This "DBS" represents the block size of the data. And "FN" (Fraction number) disposed next represents the number of blocks into which one source packet is divided. Next "QPC" (Quadlet padding count) represents the number of dummy quadlets attached. And "SPH" (Source packet header) disposed next signifies whether the source packet has a source packet header or not.

An area "Rsv" is reserved for the future, and "DBC" represents the counts value of successive data blocks for detecting the data block loss.

"FMT" represents a Format ID, and "FDF" represents a Format dependent field.

Fig. 6 shows a format of a cycle start packet. At the top of this packet, there is disposed "destnation_ID" which represents ID of a data destination. Each bit of next "tl" (transaction label) is set normally to 0. And the value of the time variable key i for example can be recorded here.

Each bit of "rt" (retry code) is set normally to 0. And a packet type transaction code is disposed in next "tcode" (transaction code).

An area "pri" stands for priority, and each bit thereof is set to 1 when used between apparatus connected mutually via the 1394 bus 5. The time variable key i can be allocated to this "pri" also.

ID of a data source is recorded in "source_ID", and a clock value corresponding to the timing deviation from the cycle start packet is set in "destination_offset". And a register value used as a reference for the cycle master as described is set in "cycle_time_data". The time base reference of the isochronous cycle of each electronic apparatus connected to the 1394 bus 5 is set with reference to this clock value. Also the CRC of the header is disposed in the last area.

In the embodiment described above, the time variable key i is transmitted after being written in the data part or the header of each packet. However, the value of "destination_offset", "cycle_time_data" or "header_CRC" in the cycle start packet may be used directly as the time variable key i.

Since each electronic apparatus reads out such values and holds the same in the registers 35 and 36 of the cycle monitor 32, it is also possible to extract the time variable key i from the values thus held.

Further, the value of "DBC" of the CIP header shown in Fig. 5 or the value of "data_CRC" shown in Fig. 4 may be used directly as the time variable key i.

Thus, according to the data transmitting apparatus and method embodying the present invention, ciphered data are packetized into packets of an isochronous mode and then are transmitted to a serial bus, whereby data transmission can be performed with enhanced security.

According to the data receiving apparatus and method embodying the invention, ciphered data obtained by depacketizing the packets of the isochronous mode are deciphered, so that the data transmitted with security can be deciphered exactly.

The data ciphered by the data transmitting apparatus are transmitted after being packetized into packets of the isochronous mode and are received by the data receiving apparatus. Consequently, it becomes possible to realize an improved data transmitting/receiving system in which enhanced security is achieved.

Although the present invention has been described hereinabove with reference to some preferred embodiments thereof, it is to be understood that the invention is not limited to such embodiments alone, and a variety of other changes and modifications will be apparent to those skilled in the art without departing from the scope of the invention as claimed.

Claims

1. An apparatus for transmitting data in a first mode and a second mode, comprising:

   a means for ciphering the data to be transmitted by the use of cipher keys;
   a means for packetizing the ciphered data into packets of the second mode; and
   a means for transmitting the output of said packetizing means.

2. The apparatus according to claim 1, wherein transmission of the data is performed in conformity with the IEEE 1394 protocol.

3. The apparatus according to claim 1, wherein said first mode is an asynchronous mode, and said second mode is an isochronous mode.

4. The apparatus according to claim 3, wherein said packetizing means attaches, to a header of the ciphered data, an identification code relative to the ciphering.

5. The apparatus according to claim 3, wherein said cipher keys consist of a session key invariable in each session of the data to be transmitted, and a time variable key updated in each session.

6. The apparatus according to claim 5, wherein information relative to the time variable key is contained in each packet of the isochronous mode.

7. The apparatus according to claim 6, wherein the information relative to the time variable key is contained in a start packet of the isochronous mode.

8. The apparatus according to claim 5, wherein information relative to the session key is contained in each packet of the isochronous mode.

9. The apparatus according to claim 6, wherein the information relative to the session key is contained in a start packet of the isochronous mode.

10. A method of transmitting data in a first mode and a second mode, comprising the steps of:

    ciphering the data to be transmitted by the use of cipher keys;
    packetizing the ciphered data into packets of the second mode; and
    transmitting the packetized output.

11. The method according to claim 10, wherein transmission of the data is performed in conformity with the IEEE 1394 protocol.

12. The method according to claim 10, wherein said first mode is an asynchronous mode, and said second mode is an isochronous mode.

13. The method according to claim 12, wherein an identification code relative to the ciphering is attached, in said packetizing step, to a header of the ciphered data.

14. The method according to claim 12, wherein said cipher keys consist of a session key invariable in each session of the data to be transmitted, and a time variable key updated in each session.

15. The method according to claim 14, wherein information relative to the time variable key is contained in each packet of the isochronous mode.

16. The method according to claim 15, wherein the information relative to the time variable key is contained in a start packet of the isochronous mode.

17. The method according to claim 14, wherein information relative to the session key is contained in

each packet of the isochronous mode.

18. The method according to claim 15, wherein the information relative to the session key is contained in a start packet of the isochronous mode.

19. An apparatus for receiving data transmitted thereto in a first mode and a second mode, comprising:

a means for receiving the transmitted data;
a means for depacketizing the output packets obtained from said receiving means; and
a means for deciphering the ciphered data outputted from said depacketizing means.

20. The apparatus according to claim 19, wherein transmission of the data is performed in conformity with the IEEE 1394 protocol.

21. The apparatus according to claim 19, wherein said first mode is an asynchronous mode, and said second mode is an isochronous mode.

22. The apparatus according to claim 21, wherein said depacketizing means separates an identification code relative to the ciphering from the received data.

23. The apparatus according to claim 21, wherein said cipher keys consist of a session key invariable in each session of the data to be transmitted, and a time variable key updated in each session.

24. The apparatus according to claim 23, wherein information relative to the time variable key is contained in each packet of the isochronous mode.

25. The apparatus according to claim 24, wherein the information relative to the time variable key is contained in a start packet of the isochronous mode.

26. The apparatus according to claim 23, wherein information relative to the session key is contained in each packet of the isochronous mode.

27. The apparatus according to claim 24, wherein the information relative to the session key is contained in a start packet of the isochronous mode.

28. A method of receiving data transmitted in a first mode and a second mode, comprising the steps of:

receiving the transmitted data;
depacketizing the output packets obtained in said receiving step; and
deciphering the ciphered data outputted in said depacketizing step.

29. The method according to claim 28, wherein transmission of the data is performed in conformity with the IEEE 1394 protocol.

30. The method according to claim 28, wherein said first mode is an asynchronous mode, and said second mode is an isochronous mode.

31. The method according to claim 30, wherein an identification code relative to the ciphering is separated from the received data in said depacketizing step.

32. The method according to claim 30, wherein said cipher keys consist of a session key invariable in each session of the data, and a time variable key updated in each session.

33. The method according to claim 32, wherein information relative to the time variable key is contained in each packet of the isochronous mode.

34. The method according to claim 33, wherein the information relative to the time variable key is contained in a start packet of the isochronous mode.

35. The method according to claim 32, wherein information relative to the session key is contained in each packet of the isochronous mode.

36. The method according to claim 33, wherein the information relative to the session key is contained in a start packet of the isochronous mode.

FIG. 1

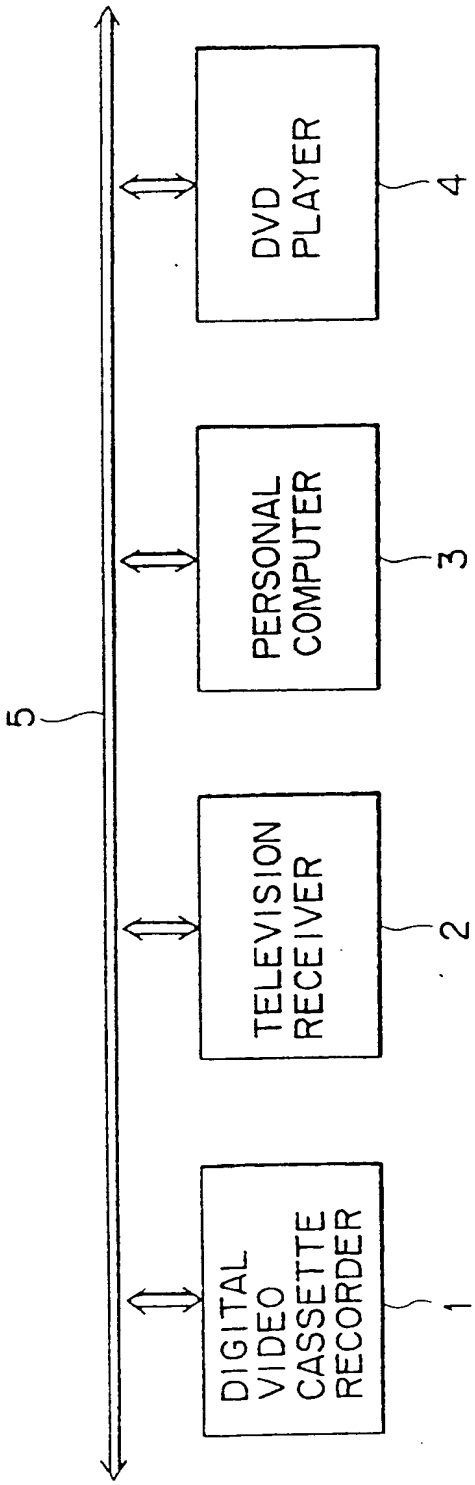

DIGITAL VIDEO CASSETTE RECORDER
1
TELEVISION RECEIVER
2
PERSONAL COMPUTER
3
DVD PLAYER
4
5

FIG. 2

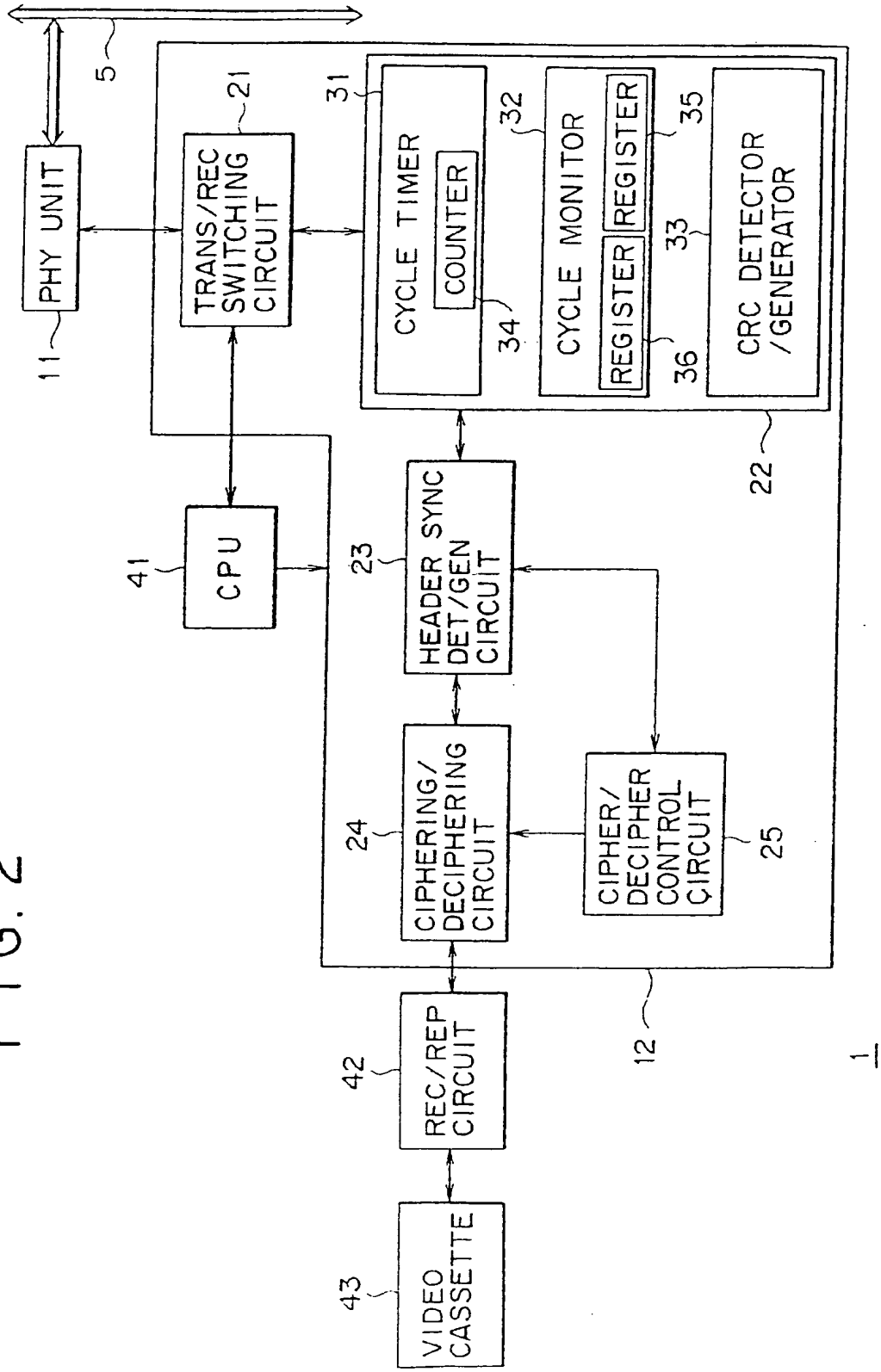

5
PHY UNIT
11
TRANS/REC SWITCHING CIRCUIT
21
CYCLE TIMER
COUNTER
31
34
CYCLE MONITOR
REGISTER
REGISTER
32
35
36
33
CRC DETECTOR /GENERATOR
22
CPU
41
HEADER SYNC DET/GEN CIRCUIT
23
CIPHERING/ DECIPHERING CIRCUIT
24
CIPHER/ DECIPHER CONTROL CIRCUIT
25
12
REC/REP CIRCUIT
42
VIDEO CASSETTE
43
1

FIG. 3

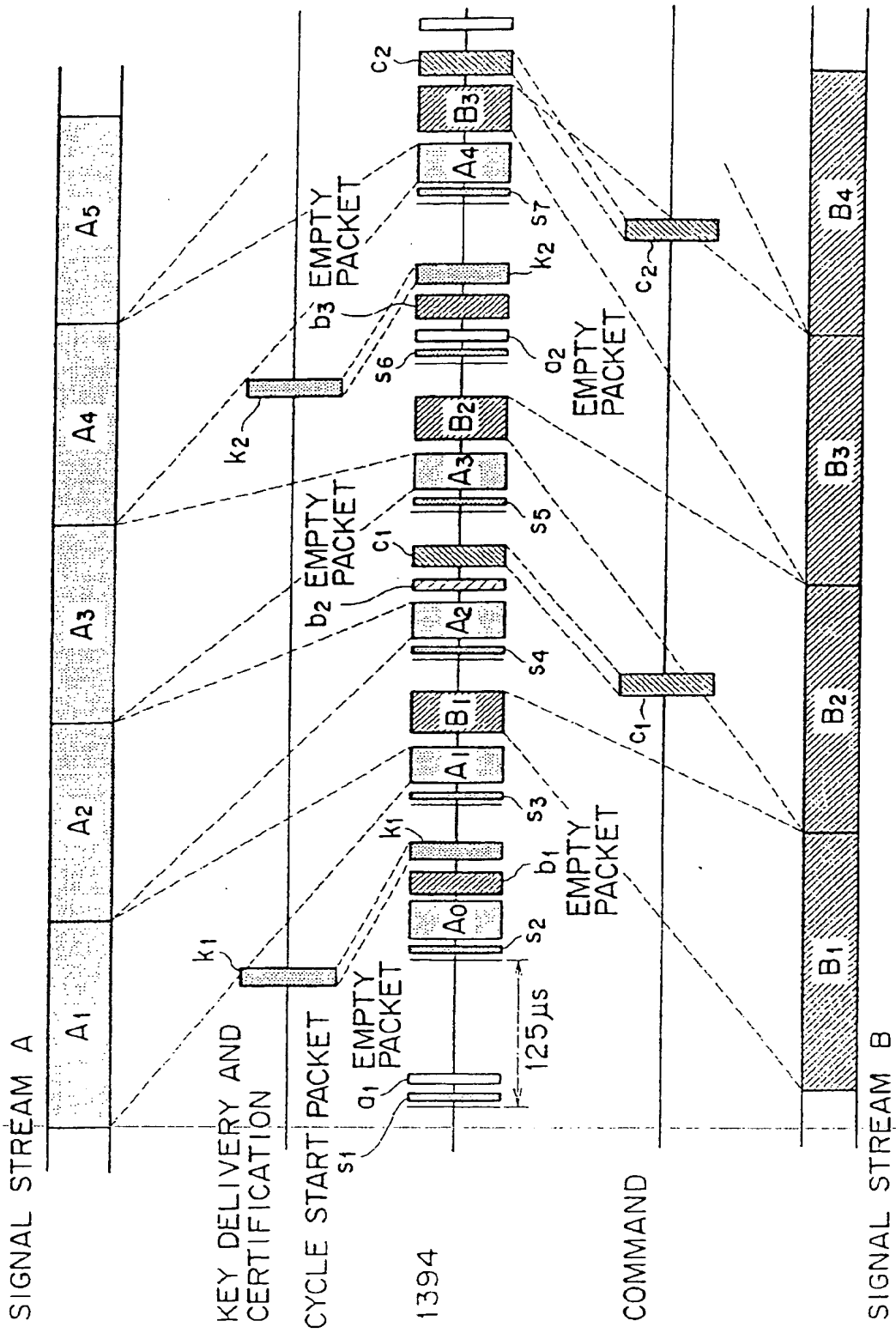
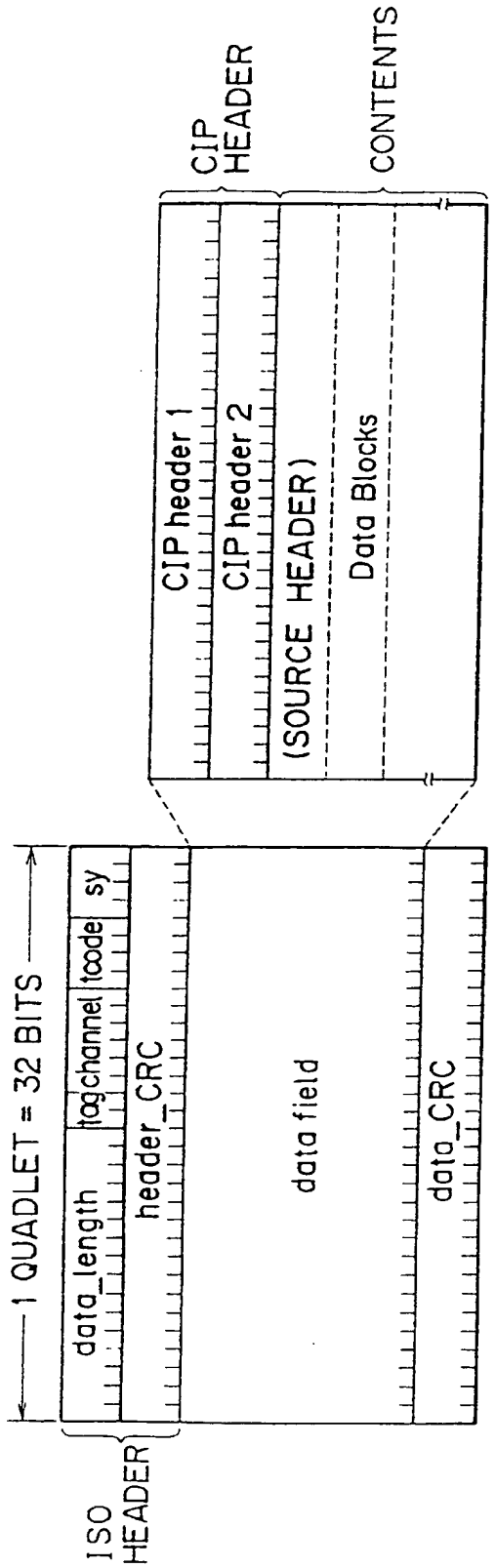

SIGNAL STREAM A
KEY DELIVERY AND CERTIFICATION
CYCLE START PACKET
1394
COMMAND
SIGNAL STREAM B
EMPTY PACKET
125μs

FIG. 4



ISOCHRONOUS PACKET

FIG. 5

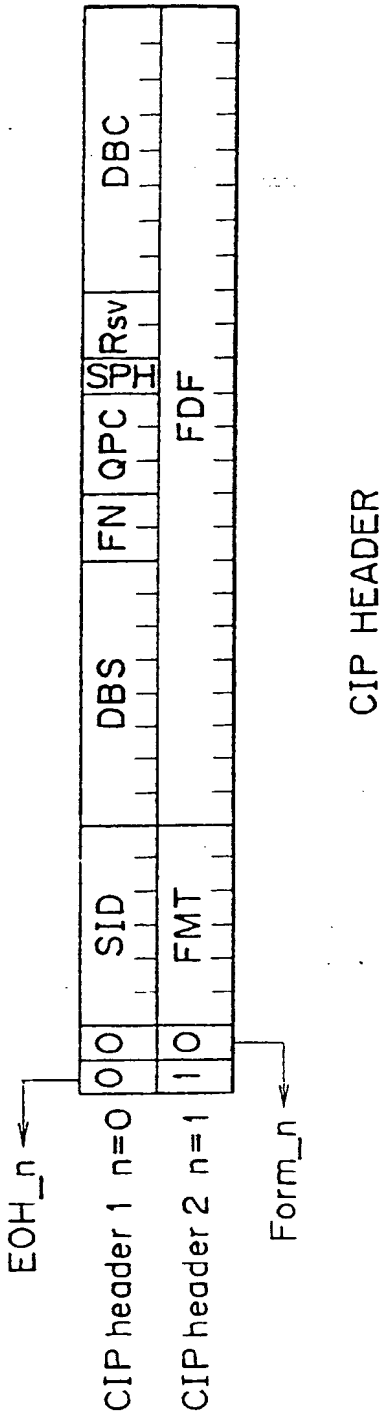
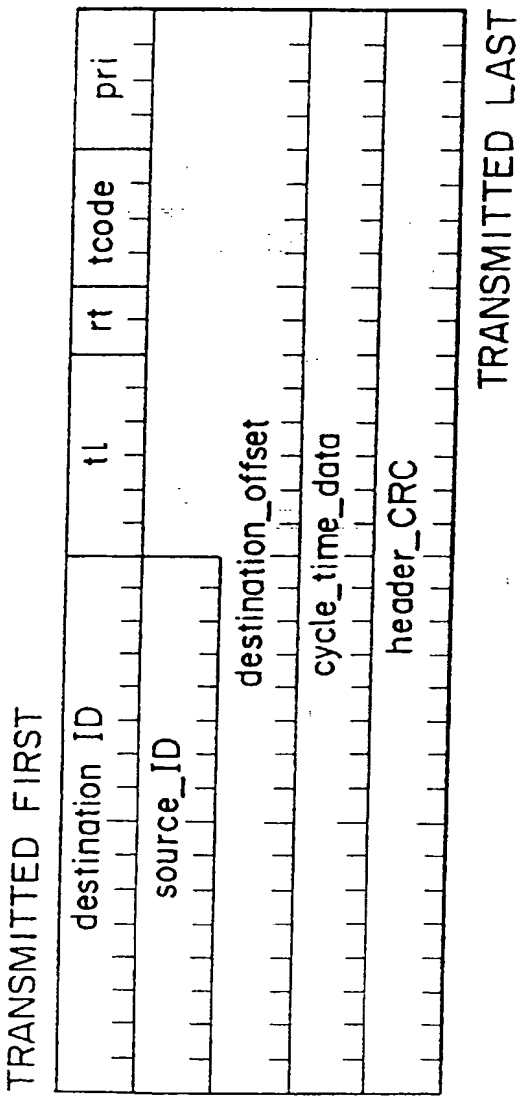

SID
DBS
FN
QPC
SPH
Rsv
DBC
FMT
FDF
0
0
1
0
CIP HEADER
EOH_n
Form_n
CIP header 1 n=0
CIP header 2 n=1

FIG. 6



CYCLE START PRIMARY PACKET FORMAT

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 874 503 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
25.08.1999 Bulletin 1999/34

(43) Date of publication A2:
28.10.1998 Bulletin 1998/44

(21) Application number: **98303004.0**

(22) Date of filing: **20.04.1998**

(51) Int Cl.[6]: **H04L 29/06**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.04.1997 JP 10610597**

(71) Applicant: **SONY CORPORATION**
Tokyo 141 (JP)

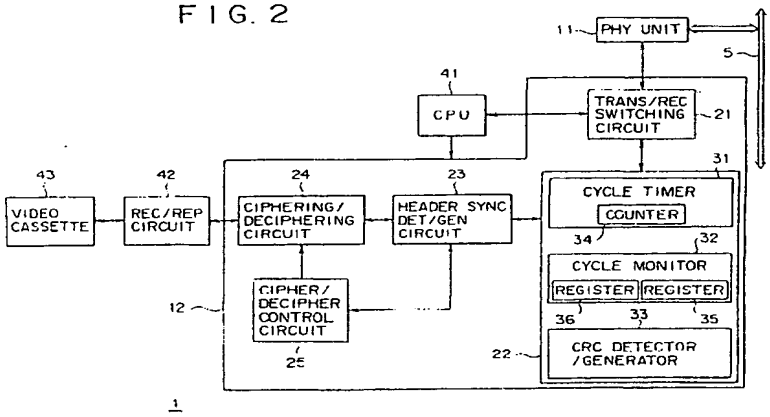
(72) Inventors:
- **Osakabe, Yoshio, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Sato, Makoto, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Osawa, Yoshitomo, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Asano, Tomoyuki, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Ishiguro, Ryuji, c/o Sony Corporation**
  Shinagawa-ku, Tokyo 141 (JP)
- **Shima, Hisato**
  Saratoga, California 95070 (US)

(74) Representative: **Pilch, Adam John Michael**
D. YOUNG & CO.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Data transmitting and/or receiving apparatus, methods and systems for preventint illegal use of data

(57) Data to be transmitted via a serial bus (5) in conformity with the IEEE 1394 protocol are ciphered by a ciphering/deciphering circuit (24), and headers are attached thereto by a header sync detecting/generating circuit (23). After further attachment of a CRC code by a CRC detector/generator (33), the data are packetized into isochronous packets of an isochronous mode by a transmission/reception switching circuit (21), whereby transmission of the data can be performed with enhanced security. Out of the cipher keys employed, a session key invariable in each session of the data is transmitted in each packet of an asynchronous mode, and a time variable key updated in each session is transmitted in each packet of an isochronous mode. The ciphered data obtained by depacketizing the packets of the isochronous mode are deciphered, so that the data transmitted with security can be deciphered exactly, and thus illegal use of the data can be prevented.

FIG. 2



EP 0 874 503 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 3004

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	EP 0 756 276 A (SONY CORP) 29 January 1997 (1997-01-29) * abstract * * column 1 - column 4, line 9 * * column 5, line 49 - column 10, line 25 * * column 11, line 52 - column 14, line 37 * * column 15, line 4 - line 26 * * figures 1-3,5-14 *	1-6,8, 10-15, 17, 19-24, 26, 28-33,35	H04L29/06 G11B20/00
Y	BLOKS R H J: "The IEEE-1394 high speed serial bus" PHILIPS JOURNAL OF RESEARCH, vol. 50, no. 1, 1 January 1996 (1996-01-01), page 209-216 XP004008212 ISSN: 0165-5817 * the whole document *	1-6,8, 10-15, 17, 19-24, 26, 28-33,35	
A	EP 0 765 061 A (HEWLETT PACKARD CO) 26 March 1997 (1997-03-26) * abstract * * page 2 - page 3, line 40 * * page 10, line 36 - page 12, line 22 * * figures 1,2,3,6A,6B,6C,7 *	1,10,19, 28	
A	KUNZMAN A J ET AL: "1394 HIGH PERFORMANCE SERIAL BUS: THE DIGITAL INTERFACE FOR ATV" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 41, no. 3, 1 August 1995 (1995-08-01), pages 893-900, XP000539552 ISSN: 0098-3063 * the whole document *	1-36	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
H04L
G11B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 July 1999	Barel-Faucheux, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 3004

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-07-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0756276 A	29-01-1997	JP 9044354 A	14-02-1997
		JP 9051343 A	18-02-1997
		CN 1148766 A	30-04-1997
EP 0765061 A	26-03-1997	US 5787483 A	28-07-1998
		JP 9172452 A	30-06-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82